AP/2136

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify that this document is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date set forth below.

by Renee D. East
Date of signature and deposit - September 6, 2007

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Benjamin J. Parker et al	Group Art Unit: 2136
Serial No.: 10/003,816	Confirmation No.: 4720
Filed: 10/25/2001	Examiner: Carl G. Colin
For: Network Security Services Architecture	Attorney Docket: 1688(15723)

****

APPELLANT'S BRIEF ON APPEAL

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the rejection of the Examiner dated June 20, 2007, which was made pursuant to reopening prosecution to enter a new ground of rejection in view of a prior Appeal Brief. Appellant has elected to initiate a new appeal. The fee for filing of a brief has already been paid.

REAL PARTY IN INTEREST

The real party in interest in the present appeal is Sprint Communications Company L.P., assignee of the entire right, title, and interest in the present application.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

STATUS OF CLAIMS

The status of the claims is as follows:

Claims allowed: none.

Claims objected to: none.

Claims rejected: 1-20.

Claims withdrawn: none.

Claims canceled: none.

The claims being appealed are: 1-20.

STATUS OF AMENDMENTS

No amendment was filed after final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention addresses the growing complexity of making available various different computer security measures to subscribers of computer networks. The invention achieves a convenient and low cost computer security system by deploying a menu of security tools within a local network that can be selected by a user connected to the network. A network architecture of the invention is structured to provide highly effective and flexible security features while greatly simplifying the user experience.

As defined in claim 1, a private network apparatus for connecting a user to an external internet comprises a plurality of security service pathways each providing a respective combination of security service features (page 6, lines 3-20; see pathways 33-37 in Figure 2). A service selection dashboard allows the user to select from a plurality of security service features for user traffic to and from the user (page 5, lines 18-31; page 9, line 12, to page 10, line 2; see steps 65-68 in Figure 4). A network management server is coupled to the service selection dashboard for storing a subscriber configuration in response to the user selected security service features (page 5, lines 24-34; AAA server 24 in Figure 2). a pass-through router couples the user traffic to the external internet independently of the security service pathways (page 5, line 35, to page 6, line 2; router 25 in Figure 2). A service selection gateway is coupled to the user for directing the user traffic to and from one of the service selection dashboard, the pass-through router, or one of the security service pathways (page 5, lines 16-23; concentrator 20 in Figure 2). A security service router couples the plurality of security service pathways to the external internet (page 6, lines 15-19; router 32 in Figure 2). The service selection gateway directs user traffic to the service selection dashboard if the subscriber configuration is in an initialized state (page 5, lines 27-29; steps 52-56 in Figure 3). The service selection gateway directs user traffic to a respective one of the security service pathways or to the pass-through router in response to the subscriber configuration after initialization by the service selection dashboard (page 10, lines 8-20; steps 57-61 in Figure 3).

Claim 14 recites a method of providing security service in a network interface to an external internet comprising the step of directing a user to a captive portal (page 9, lines 15-19; steps 52-53 in Figure 3). Security service features are presented to user (page 9, lines 28-34). A subscription profile is stored for the user in response to security service features selected by the user through the captive portal (page 9, line 37, to page 10, line 6; step 56 in Figure 3). User traffic is received from the user destined for the external internet at a service selection gateway, and then it is determined from the subscription profile which security service features to apply to the user traffic (page 10, lines 8-11;

steps 51, 57, and 60 in Figure 3). If the subscription profile for the user includes any security service features, then the user traffic is re-directed to a particular security service pathway of a plurality of security service pathways, the particular security service pathway corresponding to the security service features identified by the user profile (page 10, lines 14-20; steps 60 and 61 in Figure 3). If the subscription profile for the user includes no security service features, then the user traffic is re-directed to a pass-through router for coupling the user traffic to the external internet (page 10, lines 11-14; step 58 in Figure 3).

Claim 20 depends from claim 1 and recites a user-side switch (switch 30 in Figure 2) coupling the service selection gateway (concentrator 20 in Figure 2) to the security service pathways 33-37 (page 5, lines 16-23, and page 6, lines 8-14). An internet-side switch (switch 31 in Figure 2) is recited for coupling the security service pathways 33-37 to the security service router 32 (page 6, lines 3-18).

None of the claims contain either a means plus function or a step plus function element.

GROUNDS OF REJECTION TO BE REVIEWED

1. Whether Claims 1, 14, and 20 are unpatentable under 35 U.S.C. §102(e) as being anticipated by Ruban et al (US Patent 7,203,190).

ARGUMENT

Rejection of Claims 1, 14, and 20 under 35 USC 102(e)

Claim 1

Claim 1 recites a network architecture wherein a plurality of security service pathways each provide a respective combination of security service features. A service selection gateway directs user traffic to a respective one of the security service pathways

or to a pass-through router in response to a subscriber configuration. Consequently, a highly efficient handling of user traffic is obtained because once particular packets are sent to a security service pathway the corresponding combination of security features are automatically applied to the packets, unlike the prior art which requires routing decisions for each packet to be made at each security element in order to send it to the next security element in a combination.

Ruban fails to disclose security service pathways meeting the limitations of claim 1. The rejection equates security service pathways with "switching services" in its anticipation analysis. It erroneously relies on Ruban at column 12, lines 5-16, to show respective combinations of security service features provided in respective security service pathways. The mere switching services that are disclosed by Rubans fail to disclose all the aspects of the claimed security service pathways.

When a data packet from a user is intended to be sent to another communication network, then an interchange via a switching service (ISP or Internet Service Provider) is necessary (col. 10, lines 16-18). As described in column 11, lines 1-8, different ISP's may provide a slow and cheap switching service on one hand and a faster and more expensive switching service on the other hand. In contrast, the claimed security service pathways are within the same private network wherein a service selection gateway directs user traffic to a respective one of the security service pathways or to a pass-through router in response to a subscriber configuration. As shown by the portion of Ruban quoted by the rejection, each separate ISP has its own respective RADIUS server for authenticating and billing the user for use of the ISP. Therefore, Ruban also lacks the service selection gateway that directs user traffic to the security service pathway having the correct user-selected security service features. Thus, Ruban fails to anticipate claim 1, and the rejection should be reversed.

Claim 14

Claim 14 recites a method of providing security service in a network interface

to an external internet comprising the step of directing a user to a captive portal. Security service features are presented to user. A subscription profile is stored for the user in response to security service features selected by the user through the captive portal. User traffic is received from the user destined for the external internet at a service selection gateway, and then it is determined from the subscription profile which security service features to apply to the user traffic. If the subscription profile for the user includes any security service features, then the user traffic is re-directed to a particular security service pathway of a plurality of security service pathways, the particular security service pathway corresponding to the security service features identified by the user profile. If the subscription profile for the user includes no security service features, then the user traffic is re-directed to a pass-through router for coupling the user traffic to the external internet. Consequently, a highly efficient handling of user traffic is obtained because once particular packets are sent to a security service pathway the corresponding combination of security features are automatically applied to the packets, unlike the prior art which requires routing decisions for each packet to be made at each security element in order to send it to the next security element in a combination.

As explained above regarding claim 1, Ruban fails to disclose security service pathways wherein each pathway provides a respective combination of security service features. In Ruban, data packets may contain information items that are analyzed to identify specific path details. This information is determined from the content (header) of the data packet (col. 5, lines 18-29). Therefore, Ruban fails to teach or suggest the plurality of security service pathways of the present claims which each provide a respective combination of security service features. Upon being directed to a pathway by the service selection gateway, no further routing between security devices is necessary with the present invention since the pathway defines the security features. In contrast, Ruban consumes resources as a data packet traverses a network to maintain the data packet on the specific path.

The distribution of packets by the present invention to the correct security

service pathway having the desired combination of security service features depends upon the service selection gateway identifying the appropriate pathway and then routing a packet to the entry point of that pathway. From then on, the packet automatically passes through the selected security features. The architecture in Ruban is incapable of performing in this claimed manner. Thus, claim 14 is allowable over Ruban, and the rejection should be reversed.

Claim 20

Dependent claim 20 recites the user-side switch that couples the service selection gateway to the security service pathways, and the internet-side switch that couples the security service pathways to the security service router. These switches demultiplex traffic from separate users for processing by corresponding security service pathways and then re-multiplex the traffic for normal handling by the remainder of the network. Thus, the user-side and internet-side switches provide common entry and exit points for the parallel security service pathways. Since Ruban lacks security service pathways, it likewise fails to disclose user-side and internet-side switches as required by claim 20. Therefore, Ruban fails to anticipate claim 20, and the rejection should be reversed.

CONCLUSION

The final rejection has failed to establish anticipation of any of claims 1, 14, or 20. The prior art relied upon in the final rejection neither teaches nor suggests the structure or function of the present invention nor does it provide any teaching which can obtain the significant advantages which are achieved by the present invention. Accordingly, the rejections of claims 1-20 contained in the rejection dated June 20, 2007, should be reversed.

Respectfully submitted,

Mark L. Mollon
Registration No. 31,123
Attorney for Appellant

Date: September 6, 2007
MacMillan, Sobanski & Todd, LLC
One Maritime Plaza, Fourth Floor
720 Water Street
Toledo, Ohio 43604
Tel: 734-542-0228
Fax: 734-542-9569

CLAIMS APPENDIX

Claims 1-20 now read as follows:

1. Private network apparatus for connecting a user to an external internet comprising:

a plurality of security service pathways each providing a respective combination of security service features;

a service selection dashboard allowing said user to select from a plurality of security service features for user traffic to and from said user;

a network management server coupled to said service selection dashboard for storing a subscriber configuration in response to said user selected security service features;

a pass-through router for coupling said user traffic to said external internet independently of said security service pathways;

a service selection gateway coupled to said user for directing said user traffic to and from one of said service selection dashboard, said pass-through router, or one of said security service pathways; and

a security service router for coupling said plurality of security service pathways to said external internet;

wherein said service selection gateway directs said user traffic to said service selection dashboard if said subscriber configuration is in an initialized state; and

wherein said service selection gateway directs said user traffic to a respective one of said security service pathways or to said pass-through router in response to said subscriber configuration after initialization by said service selection dashboard.

2. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall.

3. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a virus scanner.

4. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a content filter.

5. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall and a content filter.

6. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall and a virus scanner.

7. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a content filter and a virus scanner.

8. The apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall, a content filter, and a virus scanner.

9. The apparatus of claim 1 wherein said security service pathways include at least two pathways having firewalls, said firewalls respectively providing different grades of firewall protection.

10. The apparatus of claim 9 comprising three security service pathways each including a respective firewall, said firewalls including a first firewall providing a high grade firewall protection, a second firewall providing a medium grade firewall protection, and a third firewall providing a low grade firewall protection.

11. The apparatus of claim 10 wherein said low grade firewall protection comprises port blocking for outgoing traffic.

12. The apparatus of claim 10 wherein said medium grade firewall protection comprises port blocking for incoming and outgoing traffic.

13. The apparatus of claim 10 wherein said high grade firewall protection comprises port blocking for outgoing traffic and blocking of all incoming traffic not initiated by said user.

14. A method of providing security service in a network interface to an external internet, said method comprising the steps of:

directing a user to a captive portal;

presenting security service features to said user;

storing a subscription profile for said user in response to security service features selected by said user through said captive portal;

receiving user traffic from said user destined for said external internet at a service selection gateway;

determining from said subscription profile which security service features to apply to said user traffic;

if said subscription profile for said user includes any security service features, then re-directing said user traffic to a particular security service pathway of a plurality of security service pathways, said particular security service pathway corresponding to said security service features identified by said user profile; and

if said subscription profile for said user includes no security service features, then re-directing said user traffic to a pass-through router for coupling said user traffic to said external internet.

15. The method of claim 14 wherein said security service features include firewall services, content filtering services, and virus scanning services, and wherein each of said security service pathways corresponds to a combination of said security service features.

16. The method of claim 15 wherein said firewall services comprise selectable grades of firewall protection including a high grade firewall protection, a medium grade firewall protection, and a low grade firewall protection.

17. The method of claim 16 wherein said low grade firewall protection comprises port blocking for outgoing user traffic.

18. The method of claim 16 wherein said medium grade firewall protection comprises port blocking for incoming and outgoing user traffic.

19. The method of claim 16 wherein said high grade firewall protection comprises port blocking for outgoing user traffic and blocking of all incoming traffic not initiated by said user.

20. The apparatus of claim 1 further comprising:

a user-side switch coupling said service selection gateway to said security service pathways; and

an internet-side switch coupling said security service pathways to said security service router.

EVIDENCE APPENDIX

No evidence has been submitted under 37 CFR §§1.130, §§1.131, §§1.132, or otherwise.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings and no corresponding decisions rendered.